UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/538,926	03/30/2000	Vance C. Bjorn	03022.P019	8632

			EXAMINER
7590	11/10/2003		MOORTHY, ARAVIND K

Judith A Szepesi
Blakely Sokoloff Taylor & Zafman LLP
7th floor
12400 Wilshire Boulevard
Los Angeles, CA 90025

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 11/10/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/538,926	BJORN ET AL.
	Examiner	**Art Unit**	
	Aravind K Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _10 August 2000_ .

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-23_ is/are pending in the application.

    4a) Of the above claims _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-23_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _30 March 2000_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____ .

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-23 are pending in the application.

2. Claims 1-23 have been rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

3. Claims 1-4 and 6-9 are rejected under 35 U.S.C. 102(e) as being anticipated by Shockley et al U.S. Patent No. 5,534,855.

As to claim 1, Shockley et al discloses a client requesting a cryptographic service [column 1, lines 41-48]. Shockley et al discloses establishing a secure connection between the client and a biometric certification server (BCS) [column 4 line 66 to column 5 line 35]. Shockley discloses receiving biometric data from a user. Shockley et al discloses that the BCS

performs the cryptographic service if the user is authenticated based on the biometric authentication [column 6, lines 39-49]. Shockley discloses that the BCS returns the data to the client [column 5, lines 48-58].

As to claim 2, Shockley et al discloses the cryptographic service is authenticating the user to another server [column 10 line 35 to column 11 line 48].

As to claim 3, Shockley et al discloses generating a temporary public key/private key pair for the user and certifying the public key [column 5, lines 48-58]. Shockley et al discloses forwarding the certificate to the other server [column 5 line 59 to column 6 line 19].

As to claim 4, Shockley et al discloses that the client receives data from the other server for signing with the user's private key [column 11, lines 19-40]. Shockley et al discloses forwarding the data to the BCS [column 11, lines 19-40]. Shockley et al discloses that the BCS signing the data with the user's temporary private key [column 11 line 49 to column 12 line 30].

As to claim 6, Shockley et al discloses detecting an access to a certification database of the client by another server [column 10, lines 18-34]. Shockley et al discloses inserting a temporary certification from the BCS into the certification database of the client [column 10, lines 18-34]. Shockley et al discloses generating a true certificate if the other server chooses the temporary certification [column 10, lines 18-34].

As to claim 7, Shockley et al discloses that the cryptographic service is signing or encrypting data [column 10, lines 18-34].

As to claim 8, Shockley et al discloses that retrieving a private key/public key pair for the user. Shockley et al discloses performing the cryptographic service with the private or the public key [column 6, lines 31-49].

As to claim 9, Shockley et al discloses detecting an access to a certificate database of the client, as discussed above. Shockley et al discloses detecting the user attempting to perform a cryptographic activity [column 10, lines 18-34].

As to claim 10, Shockley et al discloses receiving a request for a certificate from the server [column 11 line 49 to column 12 line 30]. Shockley et al discloses forwarding the request to a biometric certification server (BCS) [column 11 line 49 to column 12 line 30]. Shockley et al discloses receiving a biometric identification from the client and forwarding the biometric identification to the BCS [column 5 line 59 to column 6 line 8]. Shockley et al discloses that if the biometric identification matches a registered user on the BCS, receiving a certificate including a public key of the client certified by the BCS [column 5, lines 48-58]. Shockley et al discloses forwarding the certificate to the server, thereby identifying the client to the server [column 5, lines 48-58].

As to claim 11, Shockley et al discloses detecting an access to a certification database by the server, as discussed above. Shockley et al discloses inserting a temporary certification from the BCS into the certification database, as discussed above. Shockley et al discloses generating a true certificate if the server chooses the temporary certification, as discussed above.

As to claim 12, Shockley et al discloses that the BCS generates a disposable public/private key pair in response to the request [column 5, lines 48-58]. Shockley et al discloses that the BCS certifies the disposable public key of the user [column 5, lines 48-58].

4. Claims 22 and 23 are rejected under 35 U.S.C. 102(e) as being anticipated by Matyas Jr., et al U.S. Patent No. 6,507,912 B1.

As to claim 22, Matyas et al discloses a crypto-API (application program interface) for receiving cryptographic function requests [column 5, lines 5-21]. Matyas et al discloses a cryptographic service provider for establishing a secure connection to a remote crypto-server [column 2, lines 24-39]. Matyas et al discloses having the crypto-server perform the cryptographic function [column 2, lines 24-39]. Matyas et al discloses a sensor for receiving biometric data from a user [column 2, lines 24-39]. Matyas et al discloses that the biometric data is sent to the crypto-server to authenticate the user [column 2, lines 40-49].

As to claim 23, Matyas et al discloses a crypto-API (application program interface) for receiving cryptographic function requests [column 5, lines 5-21]. Matyas et al discloses a cryptographic service provider for establishing a secure connection to a remote crypto-server [column 2, lines 24-39]. Matyas et al discloses having the crypto-server perform the cryptographic function [column 2, lines 24-39]. Matyas et al discloses a sensor for receiving biometric data from a user [column 2, lines 24-39]. Matyas et al discloses that the biometric data sent to the crypto-server to authenticate the user [column 2, lines 40-49]. Matyas et al discloses that the remote crypto-server comprises: a crypto-proxy interface for receiving a request for the cryptographic function from the client on the secure connection [column 6, lines 30-52]; an authentication engine for authenticating the user based on the biometric data [column 5, lines 5-21]; a cryptographic engine for performing the cryptographic functions [column 8, lines 4-14]; and the crypto-proxy interface for returning data to the client, after the cryptographic functions are performed [column 7, lines 36-51].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

5.   **Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shockley et al**

U.S. Patent No. 5,534,855 as applied to claim 1 above, and further in view of Brickell et al

U.S. Patent No. 5,534,855.

As to claim 5, Shockley et al does not teach that the client generates a session key for use

with the other server. Shockley et al does not teach encrypting the session key with a public key

of the other server. Shockley et al does not teach that the client closes the secure connection

between the client and the BCS once the session is established between the client and the other

server.

Brickell et al teaches that the client generates a session key for use with the other server.

Brickell et al teaches encrypting the session key with a public key of the other server [column 8,

lines 31-47]. Brickell et al teaches that the client closes the secure connection between the client

and the BCS once the session is established between the client and the other server [column 8,

lines 31-47].

Therefore, it would have been obvious to a person having ordinary skill in the art at the

time the invention was made to have modified Shockley et al so that the client generated a

session key for use with the other server. The session key would have been encrypted with the

public key of the other server. The client would have closed the secure connection between the

client and the BCS once the session was established between the client and the other server

It would have been obvious to a person having ordinary skill in the art at the time the

invention was made to have modified Shockley et al by the teaching of Brickell et al because

the examiner asserts that this prevents a third party from intercepting the session key.

6. Claims 13-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shockley et

al U.S. Patent No. 5,534,855 in view of Jakobsson U.S. Patent No. 6,587,946 B1.

As to claim 13, Shockley et al discloses an authentication engine for authenticating the

user based on biometric data [column 8, lines 5-50]. Shockley et al discloses a cryptographic

engine for performing the cryptographic functions [column 8, lines 5-50].

Shockley et al does not teach a crypto-proxy interface for receiving a request for a

cryptographic function from a client on a secure connection. Shockley et al does not teach that

the crypto-proxy interface returns data to the client, after the cryptographic functions are

performed.

Jakobsson teaches a crypto-proxy interface for receiving a request for a cryptographic

function from a client on a secure connection [column 5, lines 48-64]. Jakobsson teaches that the

crypto-proxy interface returns data to the client, after the cryptographic functions are performed

[column 6, lines 3-39].

Therefore, it would have been obvious to a person having ordinary skill in the art at the

time the invention was made to have modified Shockley et al so that there would have been a

crypto-proxy interface for receiving a request for a cryptographic function from a client on a

secure connection. The crypto-proxy interface would have returned the data to the client, after the cryptographic functions was performed.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Shockley et al by the teaching of Jakobsson because it is efficient, allows tight control over actions (by the use of quorum cryptography), does not require any pre-computation phase to set up shared keys, and has a trust model appropriate for a variety of settings [column 3, lines 50-58].

As to claim 14, Shockley et al teaches that a database includes user credentials [column 10, lines 18-34]. Shockley et al teaches that the authentication engine retrieving user biometric template from the database and comparing the biometric template to the biometric data received from the user [column 11, lines 3-40].

As to claim 15, Shockley et al teaches a dynamic key generation engine for generating a temporary public key/private key pair, the key pair used for establishing a session between the client and another server.

As to claim 16, Shockley et al teaches the cryptographic engine generating a certificate including the temporary public key, certified by the cryptoserver's private key [column 5, lines 48-58].

As to claim 17, Shockley et al teaches that the dynamic key generation engine destroying the temporary key pair after the session between the client and the other server is successfully established [column 6, lines 31-66].

As to claim 18, Shockley et al suggests a user self-registration interface permitting a user to choose a handle and register a biometric template [column 5, lines 36-47].

As to claim 19, Shockley et al teaches a registration engine for receiving biometric data from the user during a registration process [column 5, lines 36-47]. Shockley teaches extracting the biometric template for the user [column 5, lines 36-47]. Shockley et al teaches a user credential database for storing the handle and the biometric template of the user [column 10, lines 18-34].

As to claim 20, Shockley et al teaches that the registration engine generates a persistent private key/public key pair [column 5, lines 48-58]. Shockley et al teaches a database for storing the persistent private key/public key pair [column 5, lines 48-58].

As to claim 21, Shockley et al teaches a database for storing a persistent private key/public key pair [column 5, lines 48-58]. Shockley et al teaches that the cryptographic engine uses the persistent private key or public key when appropriate to perform the cryptographic functions [column 6, lines 9-20].
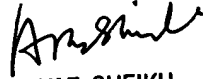
Conclusion

7.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 703-305-1373. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-1373.

Aravind K Moorthy
October 30, 2003

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100